実時間システムの仕様記述と検証に関する研究(Abstract_要旨)

AUTHOR(S):

山根, 智

氏名	山根（やまね） 智（さとし）
学位(専攻分野)	博士（工学）
学位記番号	論工博第3236号
学位授与の日付	平成9年3月24日
学位授与の要件	学位規則第4条第2項該当
学位論文題目	実時間システムの仕様記述と検証に関する研究
論文調査委員	（主査）教授 上林彌彦　教授 矢島脩三　教授 池田克夫

論文内容の要旨

本論文は，実時間システムの形式的な仕様記述と検証を対象として，検証の高速化・省メモリ化と仕様記述言語の表現能力を向上させる手法及び形式的手法のソフトウェア工学への適用方式に関する研究をまとめたものであり，以下の6章から構成されている。

第1章は緒論であり，本研究の背景，本研究の方法論を示し，本研究の目的と課題を明確にしている。形式的な仕様記述と検証の実用化の鍵は検証コストの削減や表現力の向上であり，本研究ではこれらの問題を解決するため，タイミング検証の効率化と仕様記述の高度化に着目して研究している。

第2章では，実時間システムの仕様記述と検証の基本概念を概説している。とりわけ実時間制約が表現できる時間オートマトンや実時間時相論理などの仕様記述手法及びモデル検査検証や言語包含検証などのタイミング検証手法を概観している。

第3章では，実時間時相論理による時間オートマトンのモデル検査検証手法を定式化して，タイミング検証の高速化・省メモリ化を実現させるために，実時間モデル検査検証手法及び実時間記号的モデル検査検証手法を提案している。実時間モデル検査検証手法は，時間オートマトンから時間 Kripke 構造を生成して，時間不等式手法と深さ優先探索手法で検証することにより，従来手法と比較して検証コストが約1/10に削減している。また，実時間記号的モデル検査検証手法は，時間オートマトンから時間 Kripke 構造を生成して，二分決定グラフと時間不等式手法を組み合わせた検証手法により，従来手法と比較して記憶容量が約1/100，検証時間が約1/10に削減している。

第4章では，検証の表現能力を向上させるために，確率と実時間の概念から仕様記述言語を拡張して検証する手法を提案している。本手法は，確率と実時間性の概念から仕様記述できる確率時間オートマトン及び確率実時間時相論理を提案して，従来不可能であった実時間の概念を含むランダム性を仕様記述可能としたことが特徴である。また，確率時間オートマトンから確率時間 Kripke 構造を生成して，確率実時間時相論理式を充足するかどうかを判定する確率実時間モデル検査手法を提案している。さらに，実際に検証システムを構築して，計算機実験により，実用的な検証コストで検証できることを定量的に確認して

いる。

第5章では，ソフトウェア工学で対象とする現実の複雑な実時間システムをタイミング検証するために，時間ステートチャート及び実時間オブジェクト指向による仕様記述と検証の手法を提案している。時間ステートチャートは，実時間性を含む並行プロセスや階層プロセスの集合として現実のシステムをモデル化して，視覚的かつ簡潔に，並行関係や階層関係をダイヤグラム表現するなどの特徴がある。そして，時間ステートチャートの検証については，時間ステートチャートから時間オートマトンに変換して，検証コストが大幅に削減できる言語包含検証で実現する手法を示している。また，実時間オブジェクト指向手法は，実時間性を含むオブジェクトの集合として現実のシステムをモデル化して，オブジェクトの大局的な動作モデルを時間ステートチャートで記述して検証する特徴がある。これにより，従来不可能であった実時間システムのオブジェクト指向による仕様記述と検証が可能となった。さらに，現実的な実時間システムを対象として，計算機実験により，仕様記述の簡潔性と検証コストの大幅な削減を確認している。

第6章では，本研究の成果をまとめるとともに，今後の研究課題として，モデル検査検証と証明論的検証との融合によるモジュール検証手法の研究，時間プロセス代数の時間等価性判定による検証手法の研究，述語論理に基づく実時間時相論理の研究，などの必要性を示し，将来を展望している。

論文審査の結果の要旨

本論文は，実時間システムの仕様記述と検証のための，検証の高速化と仕様記述言語の表現能力の向上に関する研究の成果をまとめたもので，得られた主な成果は次のとおりである。

(1) 時間不等式手法や二分決定グラフを使った実時間時相論理による時間オートマトンのモデル検査検証方式を提案して，タイミング検証の高速化・省記憶容量化を実現した。また，計算機実験により，従来手法に比較して，提案した手法が所要記憶容量を約1/100，計算時間を約1/10に削減できることを実証した。

(2) 確率と実時間の概念を基礎とした確率実時間時相論理，確率時間オートマトンとモデル検査検証を提案して，仕様記述と検証の表現力を向上させた。これにより，従来不可能であった実時間システムのランダム性が実用的な検証コストで，検証できることを実証した。

(3) ソフトウェア工学が対象とする複雑な実時間システムを検証可能とするために，時間ステートチャートと実時間オブジェクト指向手法を提案し，それを効率的に検証する実時間記号的言語包含検証手法を提案した。これらにより，実時間システムの仕様記述と検証が簡単になり，検証コストが大幅に削減できることが実証できた。

以上，本論文は，実時間システムに関する検証の高速化・省記憶容量化と仕様記述言語の表現能力の向上を提案したもので，学術上，実際上寄与するところが少なくない。よって本論文は博士（工学）の学位論文として価値あるものと認める。また，平成9年2月13日，論文内容とそれに関連した事項について試問を行った結果，合格と認めた。